IMPLEMENTASI ALGORITMA AES-Rijndael UNTUK ENKRIPSI DAN DEKRIPSI DATA SMS PADA PONSEL BERBASIS ANDROID

Ade Rukmana[1], Irman Nurichsan[2]
Prodi Teknik Elektro[1], Prodi D3 Teknik Telekomunikasi
Universitas Garut

Abstrak

Penelitian ini bertujuan untuk meningkatkan keamanan pesan SMS dengan menggunakan Algoritma AES-Rijndael untuk enkripsi dan dekripsi pesan masuk maupun keluar, AES mendukung berbagai variasi ukuran blok dan kunci yang digunakan yaitu 128, 192, dan 256 bit yang dibentuk dalam perangkat telepon berbasis android. Pembentukan enkripsi dan deskripsi menggunakan Java Eclipse yang dikemas dalam perangkat lunak dan memiliki antar muka yang efektif, efesien, dan tepat guna dalam penggunaanya.

Kata Kunci : Algoritma AES-Rijndael, Enkripsi, Dekripsi, *Short Message Service*, Android

Pendahuluan

Keamanan merupakan aspek yang sangat penting dalam berkomunikasi, terutama dalam masalah pengiriman dan penerimaan SMS *(Short Message Service)*. Ilmu yang mendalami teknik untuk menjaga kerahasiaan suatu data dinamakan kriptografi. Kriptografi *(cryptography)* merupakan ilmu dan seni penyimpanan pesan, data, atau informasi secara aman. Dengan melakukan enkripsi dan dekripsi menggunakan berbagai algoritma yang dirancang para kriptografer untuk menjaga kerahasiaan data *(confidentiality)*, keaslian data *(data integrity)*, otentikasi *(authentication)* serta anti penyangkalan *(nonrepudiation)*.

Seiring dengan berkembangnya teknologi komputer, dunia teknologi membutuhkan algoritma kriftografi yang kuat dan aman. Algoritma AES atau Rijndael adalah salah satu algoritma kunci simetris yang dirancang untuk memiliki property ketahanan terhadap semua jenis serangan yang telah diketahui, kesederhanaan rancangan serta kecepatan komputasi pada berbagai platform.

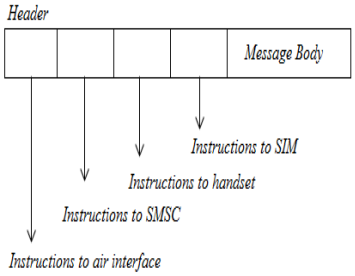
Landasan Teori

Layanan Pesan Singkat (*Short Message Service*)

Short Message Service atau yang biasa kita kenal dengan pesan singkat merupakan suatu layanan untuk mengirim dan menerima pesan tertulis (teks) dari manapun perangkat bergerak (*mobile device*). Pesan teks yang dimaksud tersusun dari huruf, angka, atau karakter alfanumerik. Pesan teks dikemas dalam satu paket/ frame yang berkapasitas maksimal 160 byte yang dapat direpresentasikan berupa 160 karakter huruf latin atau 70 karakter alphabet non-latin seperti alphabet Arab atau Cina. Hal inilah yang menjadi kelebihan SMS sebagai layanan praktis dari sisitem telekomunikasi bergerak. [Widiantoro, 2009]

Struktur Pesan SMS

Stuktur pesan pada sebuah paket SMS dapat dilihat pada *Gambar 2.1* dibawah ini :



Gambar 1 Struktur Pesan SMS

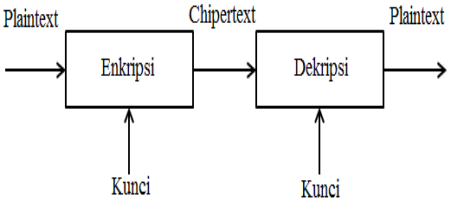
Protocol Data Unit (PDU)

Mode PDU merupakan format pesan dalam bentuk octet heksadesimal dan octet semidesinal dengan panjang mencapai 160 karakter (7 bit default alphabet) arau 140 karakter (8 bit). Kelebihan menggunakan mode PDU adalah kita dapat melakukan encoding sendiri yang tentunya harus didikung oleh hardware dan operator GSM, melakukan konversi data, menambahkan nada dering dan gambar pada pesan yang akan dikirim.

Kriptografi

Kriptografi (*cryptography*) merupakan ilmu dan seni penyimpanan pesan, data, atau informasi secara aman. Kriptografi berasal dari bahasa Yunani yaitu *Crypto* dan *Graphia* yang berarti penulisan rahasia.

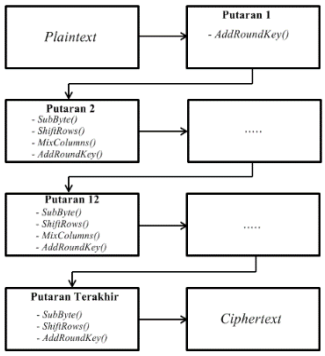
Proses transformasi dari *plaintext* menjadi *ciphertext* disebut proses *Encipherment* atau enkripsi (*encryption*), sedangkan proses mentransformasikan kembali *ciphertext* menjadi *plaintext* disebut proses dekripsi (*decryption).* Suatu pesan yang tidak disandikan disebut sebagai *plaintext* atau *cleartext.* [Firdaus, 2010]



Gambar 2 Proses Enkripsi dan Dekripsi Sederhana

***Algoritma Advanced Encryption Standard (AES)* atau Rijndael**

Algoritma AES (*Advanced Encryption Standard*) yang disosialisasikan oleh *National Institut of Standards and Technology* (NIST) pada November 2001 lahir sebagai standar baru enkripsi yang dikembangkan dari algoritma DES *(Data Encryption Standard)* melalui seleksi dengan algoritma yang lainnya. AES yang dicetuskan oleh Dr. Vincent Rijment dan Dr. Joan Daemen menjadi pemenang pada saat seleksi algoritma baru untuk menggantikan DES. Alasan utama terpilihnya AES Rijndael ini bukan karena algoritmanya yang paling aman dari *MARS, RC6, Serpent, Twofish,* dan yang lainnya, tetapi AES Rijndael memiliki keseimbangan antara keamanan serta fleksibelitas dalam berbagai *platform software* dan *hardware.*



Gambar 3 Diagram Proses Enkripsi

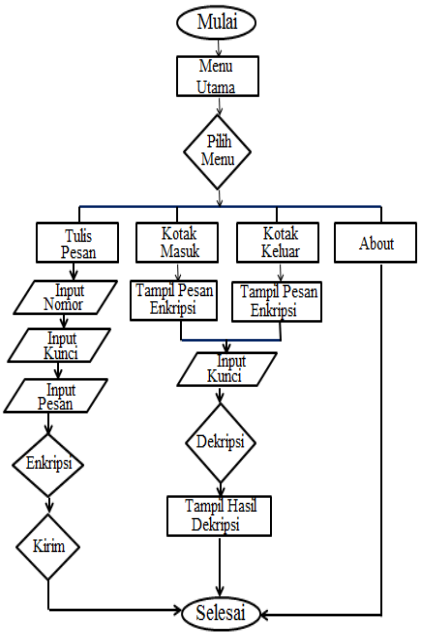
Analisis Dan Perancangan

Model proses yang digunakan dalam pengembangan sistem ini adalah model sekuensial linier. Model ini mengusulkan sebuah pendekatan pengembangan perangkat lunak yang sistematik dan sekuensial mulai dari system level dan terus maju ke analisis,

Perancangan Sistem

Desain sistem adalah suatu proses yang menggambarkan bagaimana suatu sistem dibangun untuk memenuhi kebutuhan pada fase analisis.

Flowchart Aplikasi

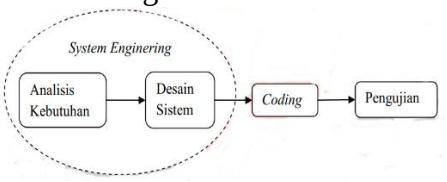


Gambar 4 *Flowchart* Pengiriman dan Penerimaan SMS

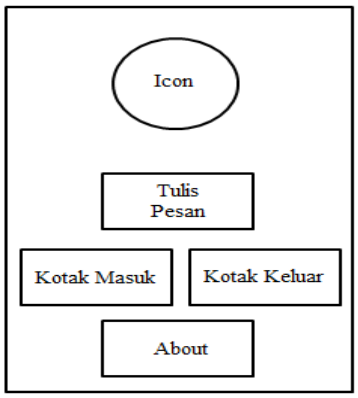
Perancangan Antarmuka

Perancangan antarmuka adalah proses desain form sebagai interaksi antara pengguna dan aplikasi. Halaman mulai ini merupakan halaman yang pertama kali muncul saat user mengklik aplikasi SMS ini, dalam halaman mulai ini terdapat beberapa menu yang digunakan untuk menampilkan tulis pesan, kotak masuk, kotak keluar dan about.

desain, implementasi, pengujian dan pemeliharaan (Pressman : 2001: 265). Model sekuensial linear melingkupi aktivitas sebagai berikut:



Gambar 5 Model Sekuensial Linier



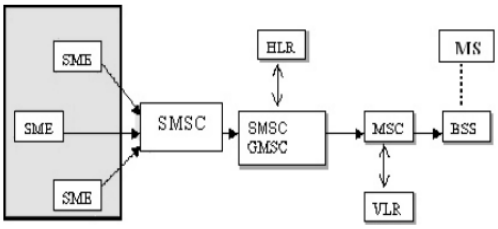
Gambar 6 Perancangan Desain Antar Muka

Implementasi Dan Pengujian

Desain Komunikasi SMS

Teknologi yang mendukung SMS antara lain adalah, GSM, TDMA dan CDMA. Dengan didukung oleh ketiga teknologi ini, SMS telah menjadi layanan data bergerak bersifat universal. Protocol yang bekerja pada SMS ini lebih dikenal dengan nama *Protocol Data Unit* (PDU).

Dalam sebuah SMSC (*Short Message Service Center*) dapat melayani berbagai macam masukan seperti *Voice Mail System (VMS), Web base messaging, Elektronic Mail (Email)* dan Eksternal SMS (ESME) lainnya. Komunikasi antara MSC dengan komponen jaringan lainnya seperti HLR dan mSC dilakukan melalui *Signal Transfer Point (STP).*



Gambar 7 Elemen-elemen pada jaringan operator selule
r

Short Message Service Center (SMSC) bertugas untuk menerima dan meneruskan pesan dari dan ke telepon seluler. SMSC dibangun oleh beberapa *Short Message Entity* (SME) yang dapat diletakan dalam jaringan atau telepon seluler. *Mobile Switching* Dalam menerima pesan dari SMSC, GMSC menggunakan jaringan SS7 (*Signaling System 7*) dalam sistem *Home Location Register* (HLR).

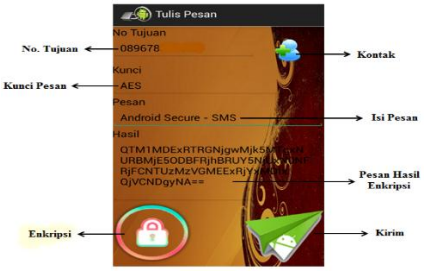
Tampilan Menu Utama

Pada menu ini terdapat empat tombol yang memiliki fungsi masing-masing yaitu, tombol tulis Pesan berfungsi untuk menuju activity tulis pesan. Tombol kotak masuk berfungsi menuju melihat daftar pesan yang telah diterima. Tombol kotak keluar berfungsi untuk melihat daftar pesan yang telah dikirim. Sedangkat tombol About berfungsi untuk melihat informasi umum pembuat program.

Gambar 10 Form Menu Utama

Form Tulis Pesan

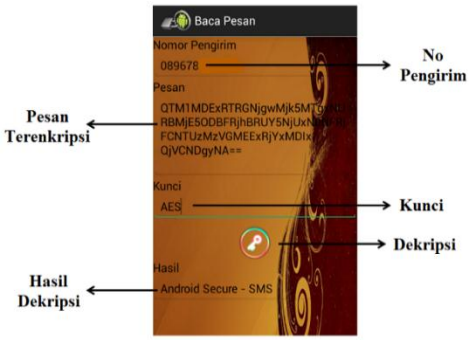
Pada tab Tulis Pesan ini pengguna diharapkan untuk memasukan nomor tujuan dengan cara mencari langsung melalui kontak, atau dapat langsung diketik pada tab yang telah disediakan, memasukan kunci pesan, pesan yang ingin disampaikan, dan menekan tombol enkripsi yang kemudian akan muncul berupa pesan hasil enkripsinya, dan kemudian pengguna dapat menekan tombol kirim pesan.



Gambar 8 Form Tulis Pesan

Form Pesan Masuk

Pada tab pesan masuk ini pengguna diharapkan untuk memasukan kunci pesan saja, dan menekan tombol dekripsi yang kemudian akan muncul berupa pesan hasil dekripsinya.



Gambar 9 Form Pesan Masuk

Pengujian Sistem

Pengujian antarmuka untuk pengirim dan penerima pesan.

- Pengiriman Pesan

Tabel 1 Pengujian Pengiriman Pesan

No	Konten	Pengujian	Hasil
1.	Penelusuran Nomor Kontak	- Pengetikan pada form input nomor. - Pencarian langsung pada kontak.	Sesuai dengan yang diinginkan, dan memudahkan dalam penelusuran kontak
2.	Input Kunci	- Pengetikan langsung pada keyboard	Sesuai, dan tetap dapat menjaga kerahasiaan kunci pesan.
3.	Tulis Pesan	- Pengetikan langsung pada keyboard	Sesuai Perancangan
4.	Enkripsi	- Mengklik langsung icon enkripsi.	Sesuai, memudahkan proses enkripsi
5.	Hasil Enkripsi	- Langsung muncul ketika kunci telah di isi dan mengklik icon enkripsi	Sesuai Perancangan
6.	Kirim Pesan	- Mengklik langsung icon kirim pesan	Sesuai Perancangan

➢ Penerimaan Pesan

Tabel 2 Pengujian Penerimaan Pesan

No	Konten	Pengujian	Hasil
1.	Input Kunci	- Pengetikan langsung pada keyboard	Sesuai, karena tetap dapat menjaga kerahasiaan kunci pesan.
2.	Dekripsi	- Mengklik langsung icon dekripsi.	Sesuai, memudahkan proses dekripsi.
3.	Hasil Dekripsi	- Langsung muncul ketika kunci telah di isi dan mengklik icon dekripsi	Sesuai Perancangan

Evaluasi Sistem dan Hasil Sistem Pengujian

Dari hasil pengujian sistem pada pengiriman SMS di atas terdapat beberapa hasil, diantaranya :

1. Karakter pesan bertambah panjang setelah dilakukan enkripsi, pertambahan karakter bergantung pada panjang pesan itu sendiri;
2. Ketika pesan asli di enkripsi, tidak memerlukan waktu lama untuk menunggu pesan hasil enkripsinya muncul. Waktu yang digunakan dalam proses enkripsi relatif singkat, yaitu tidak lebih dari 1 detik pesan hasil enkripsi akan langsung muncul pada form hasil;
3. Dan ketika ada pesan masuk, pengguna hanya tinggal memasukan kunci pesan yang sama dengan kunci pesan pengirim, kemudian mendekripsi pesan tersebut dalam waktu kurang dari 1 detik maka akan muncul pesan hasil dekripsinya pada form hasil;
4. Dalam pengujian program ini, pengiriman maupun penerimaan pesan sangat bergantung pada jaringan operator seluler itu sendri.

KESIMPULAN

Penerapan Algoritma AES-Rijndael untuk enkrpsi pesan pada pengiriman SMS (*Short Message Service*) berbasis Android dapat meningkatkan keamanan suatu pesan. Dengan variasi jenis kunci input berupa huruf, angka, simbol maupun gabungan dari ketiganya. Pesan yang terenkripsi tidak dapat dimengerti maknanya jika tidak dilakukan dekripsi pesan menggunakan kunci yang sama dengan pengirim pesan terlebih dahulu.

Dari beberapa percobaan yang dilakukan, proses enkripsi dan dekripsi pada SMS berjalan dengan baik dan hasil keluaran dari enkripsi maupun dekripsi juga sesuai sebagai mana mestinya. Waktu yang dibutuhkan dalam proses enkripsi maupun dekripsi suatu pesan tidak membutuhkan waktu lama, dalam waktu tidak lebih dari 1 detik pesan hasil enkripsi maupun dekripsi akan muncul pada form yang telah disediakan.

Saran

Pada penelitian yang saya buat ini tentu masih banyak sekali kekurangan, dan mungkin dapat disempurnakan oleh penelitian-penelitian selanjutnya. Untuk menyempurnakan program ini penulis memberikan beberapa saran diantaranya:

1. Saat ini aplikasi yang penulis buat belum terintegrasi langsung dengan operator seluler, penulis mengharapkan dalam pengembangan selanjutnya sudah terintegrasi langsung dengan operator seluler;
2. Aplikasi ini belum bisa memberikan notifikasi berita pesan terkirim, sehingga pesan yang dikirim tidak diketahui terkirim atau tidak-nya ke penerima;
3. Dan dalam pengiriman pesan, aplikasi ini belum bisa memberikan pilihan dengan *SIM-Card* mana pesan itu akan dikirimkan.

Demikian beberapa saran yang dapat dipergunakan sebagai pertimbangan untuk pengembangan aplikasi pada penelitian selanjutnya.

DAFTAR PUSTAKA

1. Ariyus, Dony. 2005. Kriptografi Keamanan Data dan Komunikasi. Yogyakarta : Andi;
2. Farid Fachrurozi, Muhamad. 2006. Enkripsi Pesan Rahasia Menggunakan Algoritma (Advance Encryption Standard) AES-Rijndael. Jakarta : UIN Syarif Hidayatullah;
3. Federal Information Processing Standards Publication 197. 2001. Announching The Advanced Encryption Standard (AES). National Institute of Standard and Technology (NIST);
4. Hermawan, Stephanus S. 2011. Mudah Membuat Aplikasi Android. Yogyakarta : Andi;
5. Pressman, R.S. 2002. Rekayasa Perangkat Lunak. Buku Satu. Edisi Terjemahan. Yogyakarta : Andi;
6. Widiantoro, Aris. 2009. Pembangunan SMS Gateway Informasi Nilai Program Pasca Sarjana Universitas Sebelas Maret Surakarta. Surakarta : Universitas Sebelas Maret ;
7. http://triwahyudingeblogyuk.blogspot.com/2010/12/ancaman-keamanan-pada-short-messaging.html diakses 28 November 2013;
8. http://eprints.mdp.ac.id/781/1/Jurnal%202008250062%20Three%20Maskes.pdf diakses 28 September 2013;
9. http://thesis.binus.ac.id/Asli/Bab2/2010-1-00594-SK%20Bab%202.pdf diakses 19 Januari 2014;
10. http://www.4shared.com/get/MyorABt6/TI_-_Kriptografi.html diakses 21 Januari 2014;
11. http://tekno.liputan6.com/read/806673/malware-terbaru-android-bisa-curi-sms-dan-panggilan-telepon diakses 21 Januari 2014.